Integrating HIPAA Into Your Compliance Program

Fifth Annual National Congress on Health Care Compliance
February 7, 2002

Glenna S. Jackson
Vice President Compliance, MedStar Health

Diane H. Meyer
Chief Privacy Officer & Senior Project Manager, Enterprise Solutions Group
Interim Privacy Officer, MedStar Health

MedStar Health
HIPAA Initiative
Protecting Patient Privacy

Just do it... COMPLIANCE right!

ENTERPRISE SOLUTIONS GROUP, INC.

Seven Elements of an Effective Compliance Program

Organization

Policy

Training

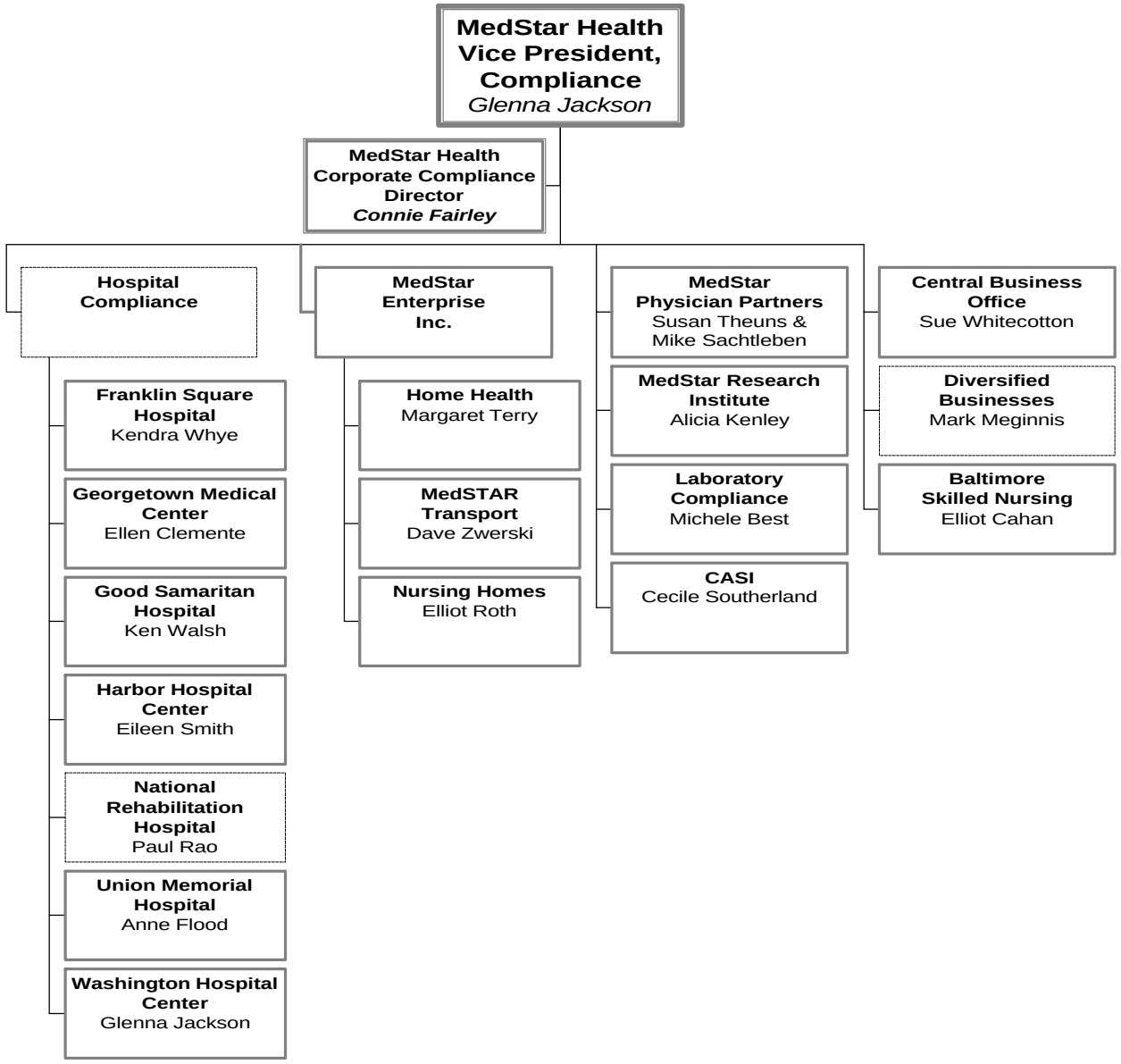
Monitoring

Communications

Responding to Concerns

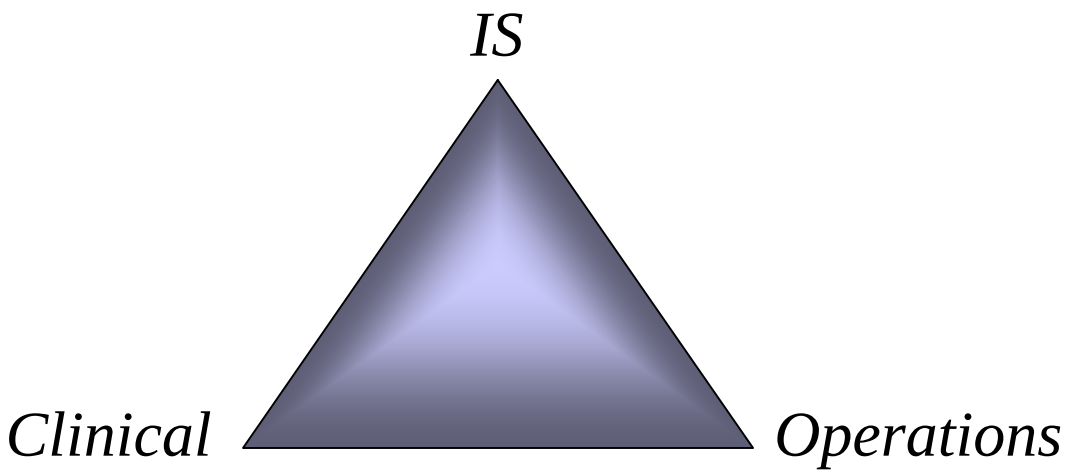
Discipline

Organization



Organization

- Expansion of existing Compliance Committee for HIPAA Implementation Process
- Once implementation is complete, Privacy Officer and Compliance Officer coordinate on-going privacy compliance management
- Key areas of representation for expanded Compliance Committee = HIPAA Implementation Task Force



Organization

Implementation Task Force Representation Considerations

- Medical Records
- Patient Financial Services
- Compliance/Risk Management
- Admissions
- Outpatient services
- IS
- Facilities
- Legal
- Marketing/Public Affairs
- Fundraising
- Operations/Planning
- Business Affairs
- Human Resources/Labor Relations
- Patient Relations
- Physicians
- Nurses/Patient Care Services
- Pharmacy
- Lab
- Residents/Teaching
- Physicians Relations
- Referrals
- Clinical - major product lines:
  - Research
  - Emergency
  - Cancer Services
  - Heart Services
  - Women's Services
  - Surgical Services
  - Radiology

Organization

- Compliance Officer
- Privacy Officer
- Security Officer
- Implementation Task Force / Expanded Compliance Committee
- Patient Privacy Advisory Council

Policy

- Code of Conduct and Compliance Policies
- Enterprise-wide policy review for privacy gap analysis – where are we now, where do we need to go?
- Modification of existing policies (examples: patient access to records, patient amendment of records, release of information for marketing purposes)
- Development of new policies (examples: accounting of disclosures, Notice of Privacy Practices, Business Associate Agreements)
- Policies for on-going compliance monitoring

Policy

Information Capture for development of the Notice of Privacy Practices

Does your department handle Protected Health Information (PHI) in any of the following ways?

- Create new PHI in electronic records
- Create new PHI in paper-based records
- Add PHI to records created by others
- Transfer PHI to another department within your hospital or business unit
- Receive PHI from another department within your hospital or business unit
- Disclose PHI to persons or entities outside your hospital or business unit
- Receive PHI from persons or entities outside your hospital or business unit
- Maintain PHI in electronic records in your department
- Maintain PHI in paper-based records in your department
- Review PHI created or compiled by others for other than treatment or payment
- Other (explain)_____
- *Not applicable: This department does not handle PHI*

Please complete the sections below only for each of the boxes checked above

Policy

Information Capture for Notice Development (continued)

- What PHI is created (added)?
- For what purpose is PHI created (added, transferred, received, disclosed, reviewed)?

Treatment___ Payment___ Other (please describe the purpose)

- To which other departments (outside entities) is PHI transferred (received)?
- How is PHI transferred (received)? (original paper-based records, copies of paper based records, fax, email, telephone, etc.)
- What specific information is transferred (received, maintained, viewed)? (clinical information, demographic information, billing information, etc.)
- How is disclosure authorized? (written patient consent, required by law or regulation, required by contract, approved by IRB, etc.)
- In what format is PHI maintained (paper-based records, electronic-based records, CD's, images, films, videotapes, etc.)
- Where is PHI maintained (in you department, in another location within the facility, off-site storage, etc.)
- How long is PHI maintained?

Policy

Policy Template

- Policy Title
- Purpose
- Policy Statement
- Scope of Policy
- Definitions
- Responsibilities
- Exceptions
- What Constitutes Non-Compliance
- Explanation and Details/Examples
- Requirements and Guidelines for Implementing The Policy
- Related Policies
- Procedures That Are Absolutely Linked To the Policy
- Legal Reporting Requirements
- Reference to Laws or Regulations of Outside Bodies
- Right To Change or Terminate Policy

Training

- Orientation Training now – begin to raise level of awareness

- Workforce training required on organization's privacy policies and procedures

- Required training conducted towards completion of implementation – if privacy policies are changed, affected workforce must be retrained

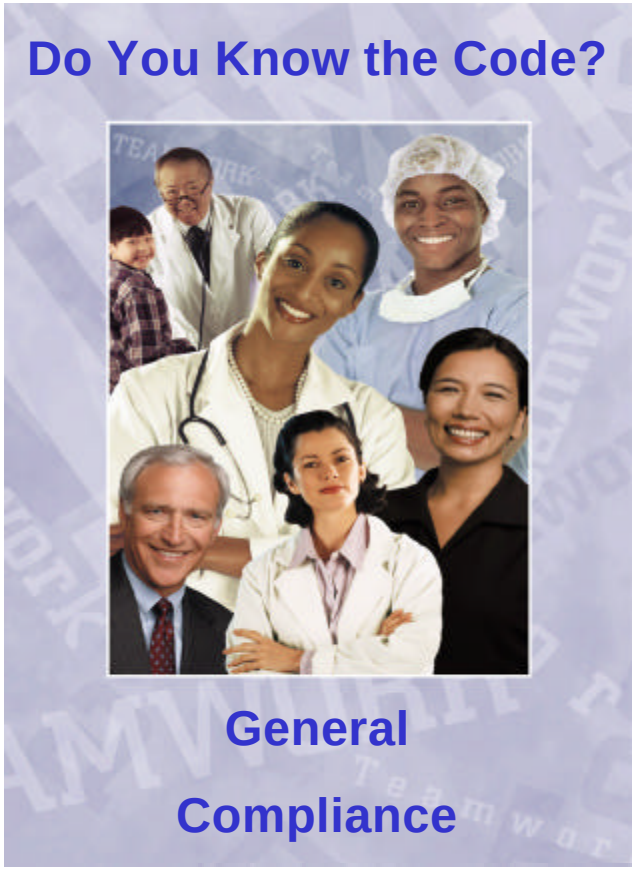
- Training customized to workforce needs – 3 levels
  - Clinical staff – staff directly involved with patient treatment
  - Staff in contact with patient information
  - Staff with minimal/no contact with patient information

- eLearning platform – if you've been considering it, now's a good time

MedStar Health

Just do it... COMPLIANCE right!

Code of Conduct
and
General Compliance



Patient Confidentiality

- MedStar Health collects information about a patient's medical condition, history, medication, and family illnesses in order to provide the best possible care.

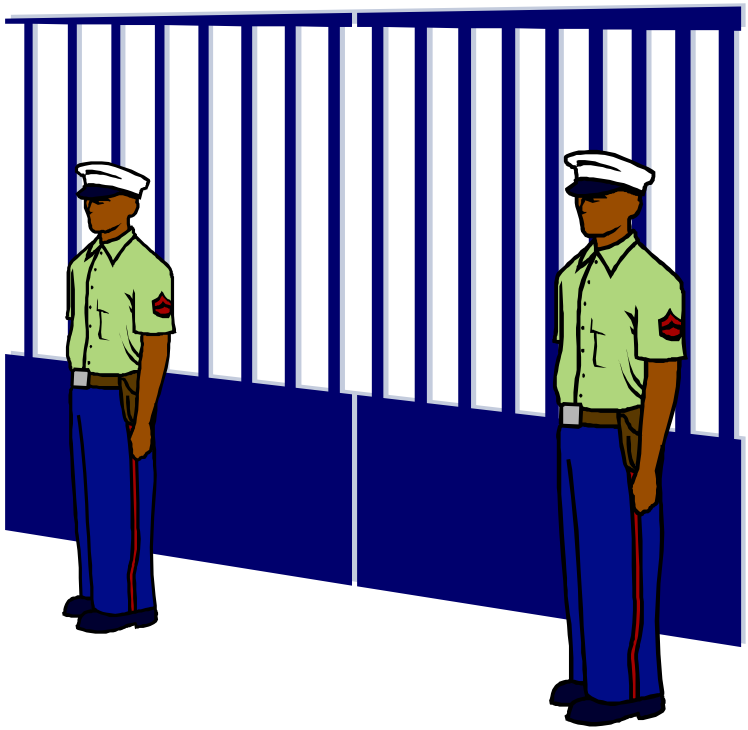
Patient Confidentiality, continued

- MedStar Health realizes the sensitive nature of patient information and is committed to maintaining its confidentiality.
- We do not release or discuss patient-specific information with others unless it is authorized by:
  - law,
  - the patient's written consent, or
  - departmental policy

What is HIPAA?

- Health Insurance Portability and Accountability Act
  - A law designed to make sure your personal health information is private and secure.

Privacy



- What does privacy mean?
  - Controlling who is allowed to get into information
  - The right to keep information about themselves from being released

Security

- What does security mean?
  - the ability to control the ways to get into information, and
  - to protect information from:
    - changes,
    - destruction
    - loss, and
    - accidental or intentional release to people who did not have permission to receive it.

HIPAA'S COVERED ENTITIES

- **Who is affected by HIPAA?**

  1) Health care entities who transmit any health information in electronic form for any of the following eight basic transactions:

- Claims
- Electronic remittance advice
- Eligibility
- Authorization
- Enrollment
- Coordination of Benefits
- Claims Status
- Premium Payments

Who is affected by HIPAA?, continued

2) Health Plans:
   - Group health plans that have fifty or more participants
   - Health insurance issuers
   - Health Maintenance Organizations (HMOs)
   - Medicare Parts A and B, Medicaid Title 19

3) Clearinghouses - includes billing services, repricing companies, community health management information systems and value added networks

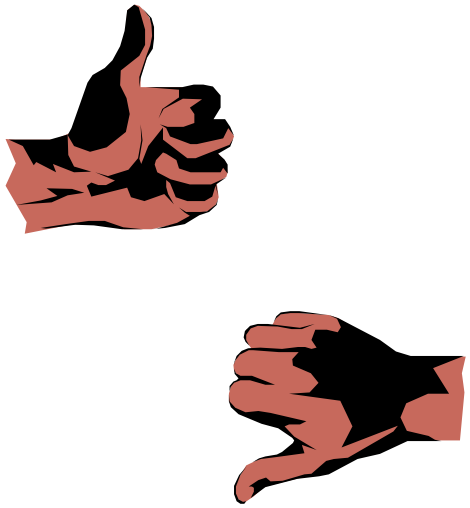
Protected Health Information

- **What does HIPAA cover?**
  - Protected Health Information (PHI)
    - Individually identifiable health information that is sent or kept in any form or medium (i.e., electronic, oral, written)

Permission to use PHI

- **Consent**
  - The patient gives permission to use and release PHI for:
    - treatment
    - payment, and
    - health care operations
- **Authorization**
  - The patient gives permission to use PHI for all other purposes.

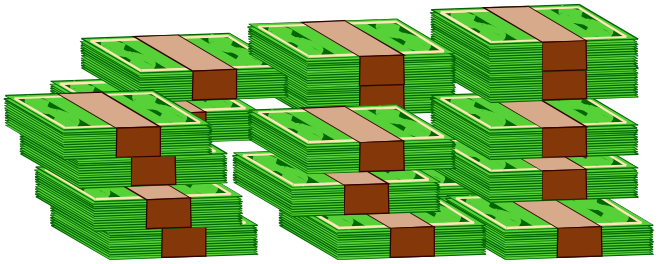
Uses & Releases Requiring an Opportunity for the Individual to Agree or Disagree



- You must provide the individual an opportunity to agree or disagree to the use and release of PHI for the following purposes:
  - Inclusion in a facility directory
  - Release to clergy
  - Release to others involved with the patient's care
  - Release to family members

Penalties

- Violations of HIPAA standards could result in the following:
  - 1-10 year jail sentence
  - $100.00-$250,000.00 in fines



Monitoring

- No external audit for HIPAA
  - Audit potential = every patient, every day
  - Internal compliance review critical

- Review for Privacy vulnerabilities before they become problematic – include patient point of view

- Similarities to OIG Work Plan and Documentation & Coding compliance review

- Similarities between Qui Tam Suits and Whistleblower provisions of HIPAA Privacy Rule

- Expand to include Business Associates, Volunteers, Vendors, Physicians not on staff

- HIPAA Enforcement Notice of Proposed Rule Making planned

- JCAHO inclusion of Privacy

Communications

- Include Patient Education - process for privacy concerns or complaints

- Establish policies and compliance review for publicity and media release

- Develop a logo and tagline

  - "Just Do It Right"

  - "Protecting Patient Privacy"

- Articles in Compliance newsletters and email updates

Responding to Concerns

- Compliance protocol for handling issues applicable to HIPAA Privacy

- Similar forms for logging complaints, ranking risk, tracking resolution

- Similar reporting process

- Hotline
  - Employees – internal compliance hotline
  - Patients – interface with customer service

- Goal is to resolve privacy issues internally
  - It is everyone's right to complain directly to HHS
  - Compliance Officer and Privacy Officer response

Discipline

- HIPAA Privacy Rule:
  - "A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures."
  - No detail provided in regulation

- Privacy violation disciplinary action policies incorporated into existing Compliance and HR policies

- Extend existing disciplinary process and mechanisms to apply to Privacy violations

- Workforce awareness of HIPAA Civil and Criminal penalties for violations of the Privacy Rule